

APIP - Cyber Liability Insurance - Coverages and Limits

The state of Washington purchases property insurance from Alliant Insurance Services through the Alliant Property Insurance Program (APIP). APIP includes a limited cyber liability insurance policy. Thus, agencies participating in the APIP property program also have cyber liability insurance. The underwriter for the cyber liability insurance policy is the Beazley Syndicate of Lloyds of London.

This document provides an overview of cyber liability policy and specific cyber liability coverages. The actual policy contains additional descriptions, definitions, and exclusions.

Policy Structure

Policy period:	10/1/2014 - 7/1/2015
Policy type:	Claims Made (e.g. covered incidents must occur and be reported within the policy period)
Coverages:	1) Financial loss recovery 2) Incident response services
Retroactive Date:	10/01/2014

Cyber Liability Policy Limits & Retention

1. \$2,000,000 per claim, \$2,000,000 annual (policy year) state of Washington aggregate limit.
2. \$25,000,000 annual APIP program aggregate limit for all participants.
3. \$100,000 retention (deductible).

Information Security & Privacy Liability Coverage (A):

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages

A claim (e.g. someone files a Tort Claim against the state) for damages and claims expense, in excess of the retention amount (deductible), which the state of Washington becomes legally obligated to pay for because of a:

- Theft, loss, or unauthorized disclosure of personally identifiable non-public information or third party corporate information in the care, custody or control of the state of Washington or an independent contractor that is holding, processing or transferring such information on behalf of the state of Washington.
- Failure of computer security to prevent a security breach including:
 - Alteration, corruption, destruction, deletion, or damage to a data asset stored on computer systems.
 - Failure to prevent transmission of malicious code from state of Washington computer systems to third party computer systems.
 - Participation by state of Washington computer systems in a denial of service attack directed against a third party computer system.
- Failure to disclose any of the above incidents in a timely manner in violation of any breach notice law.
- Failure to comply with state of Washington privacy law or agency privacy policy.
- Failure to administer an identity theft prevention program or take necessary actions to prevent identity theft required by governmental statute or regulation.

Privacy Notification Costs Coverage (B)

LIMIT: \$1,000,000 per claim/\$2,000,000 annual aggregate for all coverages (provided Beazley resources are used, otherwise only \$500,000 per claim)

Privacy notification costs, in excess of the retention amount (deductible) and incurred by the state of Washington with underwriters' prior consent resulting from a legal obligation to comply with breach notice law because of an incident or reasonably suspected incident.

NOTE: Privacy notification costs shall not include any internal salary or overhead expense of the state of Washington.

Regulatory Defense and Penalties Coverage (C)

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages

Claims expenses and penalties the state of Washington is legally obligated to pay, in excess of the retention amount (deductible), from a regulatory proceeding resulting from a violation of a privacy law caused by an incident or reasonably suspected incident.

Website Media Content Liability Coverage (D)

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages

A claim (e.g. someone files a Tort Claim against the state) for damages and claims expense, in excess of the retention amount (deductible), for which the state of Washington becomes legally obligated to pay resulting from any one or more of the following acts:

- Defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct, or other tort related disparagement or harm to the reputation or character of any person or organization.
- A violation of the rights of privacy of an individual, including false light and public disclosure of private facts.
- Invasion or interference with an individual's right of privacy, including commercial appropriation of name, persona, voice or likeness.
- Plagiarism, piracy, misappropriation of ideas under implied contracts.
- Infringement of copyright.
- Infringement of domain name, trademark, trade name, trade dress, logo, title, metatag, or slogan, service mark, or service name.
- Improper deep-linking or framing within electronic content.

Cyber Extortion Coverage (E)

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages

Cyber extortion loss, in excess of the retention amount (deductible), incurred by the state of Washington as a direct result of an extortion threat by a person, other than the state's employees, directors, officers, principals, trustees, or governors managers, members, management committee members of the management board, partners, contractors, outsourcers, or any person in collusion with any of the foregoing.

First Party Data Protection Coverage (F)

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages

Data protection loss, in excess of the retention amount (deductible), for data loss by the state of Washington as a direct result of alteration, corruption, destruction, deletion or damage to a data asset, or the inability to access a data asset that is a direct result of a failure of computer security to prevent a security breach.

First Party Network Business Interruption Coverage (G)

LIMIT: \$2,000,000 per claim/\$2,000,000 annual aggregate for all coverages

Business interruption loss, in excess of the retention amount (deductible), for income loss and extra expenses during a period of restoration following a network interruption that is directly caused by a failure of computer security to prevent a security breach.

Definitions

Breach Notice Law means any state, federal or foreign statute or regulation that requires notice to persons whose personally identifiable non-public information was accessed or reasonably may have been accessed by an unauthorized person.

Claims Made means that this policy will pay out when an incident first takes place on or after the retroactive date (10/1/2014); and before the end of the policy period; and is discovered by the state of Washington and reported to Beazley. The retroactive date will most likely be constant for all future years this policy is in force.

Computer Systems means computers and associated input and output devices, data storage devices, networking equipment, and back up facilities operated by and either owned by or leased to the state of Washington; or systems operated by a third party service provider and used for the purpose of providing hosted computer application services to the state of Washington or for processing, maintaining, hosting or storing the state of Washington's electronic data, pursuant to written contract with the state of Washington for such services.

Data Asset means any software or electronic data that exists in computer systems and that is subject to regular back up procedures, including computer programs, applications, account information, customer information, private or personal information, marketing information, financial information and any other information necessary for use in the state of Washington's ordinary course of business.

Extortion Threat means a threat to breach computer security unless an extortion payment is received. The extortion threat may seek to:

- Alter, destroy, damage, delete or corrupt any data asset.
- Prevent access to computer systems or a data asset, including denial of service attack or encrypting a data asset and withholding the decryption key for such data asset.
- Perpetrate a theft or misuse of a data asset on computer systems through external access.
- Introduce malicious code into computer systems or to third party computers and systems from state computer systems.
- Interrupt or suspend computer systems.

Incident means an act or reasonably suspected act that results in a:

- Theft, loss, or unauthorized disclosure of personally identifiable non-public information or third party corporate information in the care, custody or control of the state of Washington or an independent contractor that is holding,

processing or transferring such information on behalf of the state of Washington.

- Failure of computer security to prevent a security breach including:
 - Alteration, corruption, destruction, deletion, or damage to a data asset stored on computer systems.
 - Failure to prevent transmission of malicious code from state of Washington computer systems to third party computer systems.
 - Participation by state of Washington computer systems in a denial of service attack directed against a third party computer system.
- Failure to timely disclose any of the above incidents in violation of any breach notice law.
- Failure to comply with state of Washington privacy law or agency privacy policy.
- Failure to administer an identity theft prevention program or take necessary actions to prevent identity theft required by governmental statute or regulation.

Malicious Code means any virus, Trojan horse, worm or any other similar software program, code or script intentionally designed to insert itself into computer memory or onto a computer disk and spread itself from one computer to another.

Privacy Notification means the following reasonable and necessary costs incurred by the state of Washington within one year of the reporting of the incident or suspected incident to the underwriters.

- To hire computer security experts to determine the existence and cause of any security breach and the extent to which non-public information was accessed.
- Fees charged by an attorney to determine the applicability of and actions necessary to comply with breach notice laws.
- Provide notification to; individuals who are required to be notified by the state of Washington in applicable breach notice law.
- At the underwriters discretion, to individuals affected by an incident in which their personally identifiable non-public information has been subject to theft, loss, or unauthorized disclosures in a manner which compromises the security or privacy of such individual by posing a significant risk of financial, reputational or other harm to the individual.
- Provide up to \$50,000 for the costs of a public relations consultancy for the purpose of averting or mitigation material damage to the state of Washington reputation.
- Provide, at the underwriter's discretion, one year of credit monitoring services to those individuals whose personally identifiable non-public information was compromised. Also, mailing and other reasonable third party administrative costs associated with credit monitoring services.